National Infrastructure Protection Center
NIPC Daily Open Source Report
for 17 January 2003

Current Nationwide Threat Level is

For info click here
www.whitehouse.gov/homeland

Daily Overview

- Reuters reports Venezuelan officials have accused striking oil workers of sabotaging oilfields, refineries, and computer systems during the six−week−old strike that has brought the industry to its knees. (See item 1)
- The Midland Daily News (TX) reports the Occupational Safety and Health Administration and the Dow Chemical Co. have formed an alliance to promote worker safety and health. (See item 4)
- The Washington Post reports thousands of radioactive devices, currently used in medicine and industry worldwide, are powerful enough to inflict major damage if used by terrorists in a "dirty bomb." (See item 22)
- The CERT Coordination Center has issued vulnerabiility note VU#284857 announcing ISC has discovered several buffer overflow vulnerabilities in their implementation of DHCP (ISC DHCPD). These vulnerabilities may allow remote attackers to execute arbitrary code on affected systems. (See item 24)
- International Data Group reports Microsoft and mobile phone operator Orange are working to patch a security bug that affects the first mobile phone to use Microsoft's Windows Powered Smartphone software. (See item 27)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 16, Reuters* — **Venezuela alleges oil sabotage. Embattled Venezuelan officials on Sunday accused striking oil workers of sabotaging the country's energy industry, while assuring fellow OPEC states the government would restore output swiftly.** State oil company chief Ali Rodriguez said he would start criminal prosecutions against workers he said had sabotaged oilfields, refineries and computer systems during the six−week−old strike that has brought the industry to its knees. "There are criminal and civil cases to answer in this and of course we will apply the law in Venezuela," Rodriguez told a press conference after an OPEC meeting in the Austrian capital. Striking executives of Petroleos de Venezuela, many of whom have now been sacked by Rodriguez, say incompetence by replacement workers is to blame for a recent spate of accidents, including oil spills in the western Lake Maracaibo. The Organization of the Petroleum Exporting Countries met on Sunday in emergency session to deal with the Venezuelan stoppage, lifting quotas by 1.5 million barrels a day, seven percent. OPEC President Abdullah al−Attiyah said OPEC was hopeful that Venezuela would return to full production soon and said the other cartel members would reverse the hike when that happened. Oil Minister Rafael Ramirez said oil output should rise to two million barrels per day by the end of January and 2.5 million by mid−February. Asked if Venezuela would pump its full 2.8 million bpd quota by the end of February, **Rodriguez replied: "Not totally because damage has been very great and we don't know if there has been sabotage in some wells, so we have to be very careful." "There has been electronic sabotage and sabotage on valves because the campaign is aimed at causing accidents, and we have to take anti−sabotage measures to start up safely," said Rodriguez, a former OPEC secretary−general.** The country's main oil refineries have ground to a virtual halt, export terminals have drastically reduced loadings and long lines have formed at gasoline stations, while Venezuela resorts to importing fuel.
Source: http://abcnews.go.com/wire/Business/reuters20030112_323.html

2. *January 16, The Wall Street Journal* — **Regulators aim to lift profits in transmission of electricity. Federal energy regulators are moving to make the electric−transmission business more profitable, both to boost badly needed investment and to force structural change that they believe will make the deregulated power market healthier.** The Federal Energy Regulatory Commission (FERC), in a proposed order, said it wants to give a fat 1.5 percentage−point increase in the return on equity to transmission companies that aren't associated with utilities. It will boost the return by an additional half a percentage point if those companies cede operational control of their lines to regional grid organizations, such as the Midwest Independent Transmission System Operator Inc. **The latest order shows that FERC is no longer content just to push utilities to join grid−running organizations. "We're sending a strong signal that we want full divestiture and are willing to reward those who do so," said FERC Commissioner Bill Massey.** The commission also intends to boost financial rewards for those firms that make upgrades to power systems, either through power−line additions or by employing new technologies that don't involve wires.
Source: http://online.wsj.com/article/0,,SB104267359319966454 4,00.html?mo d=ec onomy_lead_story_lsc −

3. *January 15, Akron Beacon Journal (OH)* — **FirstEnergy almost ready to refuel Oak Harbor nuclear power plant. Davis−Besse will get fueled again, perhaps as early as Friday – the**

refurbished Ohio nuclear power plant is scheduled to be refueled at the end of this week in preparation for coolant−leak tests, owner FirstEnergy said on Tuesday. But while the fuel rods will be in place, no nuclear reactions will take place inside the reactor, the Akron utility said. Instead, the fuel rods are needed to be in place to help with a week−long test that will begin March 1 to see if nozzles at the bottom of the reactor are leaking coolant, FirstEnergy spokesman Todd Schneider said. The refueling could be delayed by a couple of days to allow additional work to take place near the reactor, he said. **FirstEnergy remains on schedule to have the nuclear plant, in Oak Harbor east of Toledo along Lake Erie, ready to be restarted by April 1, he said.**
Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id= 3572051

[Return to top]

Chemical Sector

4. *January 16, The Midland Daily News (TX)* — **Dow, OSHA form alliance. Dow and Occupational Safety and Health Administration (OSHA) have formed an alliance to promote worker safety and health, the first between the regulatory agency and a chemical company.** The agreement was signed Monday in Washington, D.C., by John Henshaw, administrator of the Occupational Safety and Health Administration of the U.S. Department of Labor, and Sam Smolik, vice president of environment, health and safety for the Dow Chemical Co. Dow is the first company in the chemical industry and the first Fortune 100 company to forge an alliance with OSHA. "This alliance with the Dow Chemical Company helps establish a solid foundation that we can build upon to further enhance a culture of prevention in the chemical industry," Henshaw said. "It's an excellent opportunity to partner with stakeholders and do all we can do to improve worker safety." Smolik said, "This alliance is all about keeping people safe. Working closely with OSHA increases our overall efficiency and is a great way to share our best practices." **Dow and OSHA will work to reduce exposure to musculoskeletal hazards; improve safety and health programs in the workplace; and provide technical knowledge and guidance on PSM. OSHA's PSM standard establishes requirements to prevent or minimize the potential for fire or explosion caused by dangerous chemicals.** The alliance encourages Dow worksites and personnel to act as industry liaisons for OSHA's cooperative programs and compliance assistance specialists.
Source: http://www.ourmidland.com/site/news.cfm?BRD=2289 ewsid=6691775>

5. *January 15, Pasadena Citizen Online (TX)* — **Residents to start petition. The Pasadena City Council adopted a resolution Tuesday to oppose the San Jacinto Rail's proposed rail line, and also encourage industry officials to hammer out an agreement preventing the construction of an additional route.** District H Councilman J.J. Isbell, who represents the affected residents, said the city's show of support for the south−side neighborhoods will assist them in the battle to keep the rail from crossing through Pasadena. **Pasadena Mayor John Manlove said the primary concern with the construction of the rail line is safety. Rail cars transporting hazardous chemicals would come within a quarter−mile of homes, schools and businesses.** "This will adversely affect a lot of people," Gauntt said. "It will affect many more people than homeowners; it'll affect the value of homes and the quality of life." **The resolution supports Bayport Industrial District shippers reaching an agreement that will negate the need for the rail line. ATOFINA Petrochemicals Inc., Bassell USA Inc.,**

Equistar Chemicals LP and Lyondell Chemical Company offered to fund the project in an effort to secure competitive rail prices. Currently, Union Pacific is the only rail to service the industries, and shippers have complained that the rates are sky high. Manlove has contended the conflict lies between Union Pacific and the shippers, and has said the agencies should be able to reach a price settlement to eliminate the need for the proposed rail line through Bayport.
Source: http://www.zwire.com/site/news.cfm?newsid=67002451fi=6

[Return to top]

Defense Industrial Base Sector

6. *January 15, DefenseNews* — **Pentagon seeks $20 billion more in 2003 to pay for war on terror.** The U.S. Defense Department is preparing to ask Congress for an extra $20 billion for 2003 to cover the cost of the war on terrorism, senior Pentagon officials said Jan. 15. **The emergency supplemental spending request would help pay for Operation Enduring Freedom in Afghanistan and costs associated with Operation Noble Eagle, initiated after the Sept. 11, 2001, terrorist attacks to help defend the U.S. homeland. The 2003 defense budget is $379 billion.** Congressional aides said they expect to receive the request in February. But Pentagon officials said they must get White House approval before submitting the emergency spending bill. A senior Pentagon official said White House budget officials are likely to whittle the Pentagon request down to about $12 billion to $14 billion before sending it to lawmakers. **In tandem, senior military planners are secretly preparing a second supplemental package to pay for a possible war with Iraq, Pentagon officials said. That supplemental request is likely to be at least $30 billion, the senior Pentagon official said. Until supplemental spending is approved, the military services must borrow from other accounts to pay for the military build−up in the Gulf region, estimated to cost between $9 billion and $13 billion, according to a September Congressional Budget Office report.** However, an aide to a member of the Senate Appropriations defense subcommittee said lawmakers are expecting a request in February for an additional $5 billion to $10 billion to help cover the cost of preparations for possible war with Iraq.
Source: http://www.defensenews.com/pgt.php?htd=i_story_1499466.htmlorldwide

7. *January 15, InsideDefense.com* — **Citing al Qaeda manual, Rumsfeld re−emphasizes web security.** Defense Secretary Donald Rumsfeld yesterday issued a message directing military component heads to redouble Internet security efforts to prevent enemies such as al Qaeda from gaining access to sensitive information. **Rumsfeld says "for official use only" and other sensitive, unclassified information −− including concepts of operations, operational plans and standard operating procedures −− "continues to be found on public Web sites," indicating that too often data posted by DOD "are insufficiently reviewed for sensitivity and/or inadequately protected. "Over 1,500 discrepancies were found during the past year," he writes. Accordingly, Rumsfeld directs that DOD component heads must increase Internet operational security efforts to ensure enemies cannot benefit from publicly available information. He reiterates official DOD policy on Internet security and dictates that it be followed in conjunction with broader policies on information release and review.** Using the OPSEC process (a system of identification and protection of critical information which is neither classified nor trade secret) in a "systematic way" and "thinking about what

may be helpful to an adversary prior to posting any information to the Web could eliminate many vulnerabilities," he writes. "Limiting details," for one thing, "is an easily applied countermeasure that can decrease vulnerabilities while still conveying the essential information," the message adds. **Component heads are directed to ensure Web site owners take responsibility for the information they post. Web site owners, for their part, must ensure a valid need exists to post their information.**
Source: http://ebird.dtic.mil/Jan2003/e20030116146940.html

[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

8. *January 16, Washington Post* — **Security official to turn focus to other transportation modes.** After a year spent racing to improve airport security, the head of the Transportation Security Administration said Wednesday that the agency will pay more attention to securing railways, buses, ports and pipelines. The TSA, which was created after the terrorist attacks Sept. 11, 2001, has been credited with improving the screening of passengers and luggage in the past year. Security experts and government officials point out that loopholes remain in areas such as air cargo security. **James M. Loy, chief of the agency, said now that the agency has met 36 deadlines over the past year to improve airport security, he is assigning officials to start pilot programs to improve security of the nation's highways, railways, ports and pipelines, which are also under the agency's mandate but have not received as much attention.** "Inconsistent security measures will only direct terrorists from one transportation mode to another with lesser security," Loy said in a speech Wednesday to transportation officials gathered in Washington. "And it cannot happen in our nation that one mode or one dimension of our system, due to neglect, finds itself as the abandoned mode. We must make sure we have consistency across our entire mode network of our national transportation system." For example, Loy said **the TSA is starting a pilot program at ports in Miami and Vancouver this year to screen cruise ship passengers' luggage at an off−site location before those passengers board airplanes. He said his agency is launching a national program on intermodal preparedness for terrorism, a program under which the TSA would work with local and state agencies to develop response drills in the event of a terrorist attack.** Loy also said **he wants to improve and expand the Transportation Worker Identification Credential**, a pilot program for airport workers who have access to secure areas of the airports.
Source: http://www.washingtonpost.com/wp−dyn/articles/A62934−2003Jan15

9. *January 16, Government Computer News* — **FAA CIO says security system development tops 2003 priorities. The Federal Aviation Administration (FAA) this year intends to develop mission support systems and boost cybersecurity within the enterprise architecture it created last year**, said Daniel Mehan, assistant administrator and CIO at FAA.

The agency also plans to improve its Web site, data management and cybersecurity, among its other IT priorities for 2003, Mehan said. FAA has consulted focus groups to figure out how to improve its Web site and make it more user−friendly. It also is working with the White House Critical Infrastructure Protection Board to adhere to national standards for cybersecurity, Mehan said. **FAA is working with the Transportation Security Administration to begin a smart−card pilot this year and develop a public−key infrastructure.** "We hope to do [the pilot] before the end of the year," he said. **FAA also will look for ways to improve cybersecurity for wireless devices.**
Source: http://www.gcn.com/vol1_no1/daily−updates/20884−1.html

[Return to top]

Postal and Shipping Sector

10. *January 16, Washington Post* — **Tests show no anthrax at postal facility.** Fears of anthrax contamination in a package sent to the Federal Reserve Board in Washington, DC were defused Wednesday by officials who said **additional tests on samples taken from the item and extensive tests of the postal facility it passed through turned up negative.** The Northeast Washington facility, where U.S. government mail is sorted, reopened Wednesday night after being shut since Tuesday evening. By Wednesday evening, technicians had collected 86 surface and air samples from automated and manual sorting machines, as well as from mail sacks and cases in the facility in the 3000 block of V Street NE and tested them. All came back negative, postal officials said.
Source: http://www.washingtonpost.com/wp−dyn/articles/A63224−2003Jan15.ht ml

11. *January 16, General Accounting Office* — **Aviation safety: undeclared air shipments of dangerous goods and DOT's enforcement approach.** The General Accounting Office (GAO) released its January 2003 report to the Ranking Minority Member, Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives on Aviation Safety: Undeclared Air Shipments of Dangerous Goods and DOT's Enforcement Approach. **When shipments of dangerous goods (hazardous chemical substances that could endanger public safety or the environment, such as flammable liquids or radioactive materials) are not properly packaged and labeled for air transport, they can pose significant threats because there is little room for error when something goes wrong in flight.** To better understand the risks posed by improper ("undeclared") air shipments, the GAO assessed what is known about their nature and frequency, what key mechanisms are in place to prevent their occurrence, and what the Department of Transportation (DOT) and the Postal Service do to enforce federal regulations for shipping dangerous goods by air. Having completed its study, the GAO recommends that DOT improve its enforcement approach by (1) determining whether the unique characteristics of air transport warrant the development of a legislative proposal that would enhance DOT's authority to inspect packages shipped by air and (2) requiring FAA to strengthen its policy on documenting the reasons for changes to the amounts of recommended fines.
Source: http://www.gao.gov/new.items/d0322.pdf

12. *January 16, Bay City News* — **Surprise inspections held at Port of Oakland. As part of California's anti−terrorist efforts, the California Highway Patrol (CHP) reported that a**

special task force assembled at the Port of Oakland Thursday morning to inspect big−rig trucks for dangerous or illegal materials. At 7:30 a.m., Thursday, members of the CHP, the United States Coast Guard, and the Oakland Port Authority began checking drivers for proper documentation, and searching through all cargo leaving the port. K−9 units are also on scene to detect explosives. CHP Sgt. Wayne Ziese says that Thursday's inspections are part of an ongoing effort to increase state and national security after the terrorist attacks of September 11, 2001.
Source: http://abclocal.go.com/kgo/news/011603_nw_chp_checks.html

13. *January 15, U.S. Environmental Protection Agency* — **U. S. EPA and U.S. Customs Service sign agreement to share information on hazardous waste, chemical, pesticide imports. The U.S. Environmental Protection Agency (EPA) and the U.S. Customs Service today signed a broad memorandum of understanding (MOU) in which the two agencies agree to share information related to the import of products regulated by a number of environmental laws.** The MOU will further EPA's ability to monitor and enforce compliance with federal environmental laws and regulations pertaining to chemical substances, pesticides, hazardous waste, and ozone−depleting chemicals, and **will enhance the nation's homeland security efforts by increasing intelligence sharing between the two agencies.** Operating under the MOU, Customs will provide EPA access in the future to its confidential Automated Commercial System (ACS), which includes information relating to the names and addresses of importers, consignees, shippers, manufacturers, quantity and value of the imported merchandise and wastes, as well as corresponding Harmonized Tariff System (HTS) codes, which will enable EPA to identify classification data for all merchandise imported into the United States. Customs also will provide EPA with specific information related to, among others, chemical substances, pesticides, hazardous waste, and ozone−depleting chemicals on a routine basis, as well as on an as−needed and emergency basis, and allow EPA to share information with federal, state, foreign and local partners as permitted by law, under strict confidentiality requirements.
Source: http://yosemite.epa.gov/opa/admpress.nsf/b1ab9f485b098972852562e7004dc686/ef3ff91ca9a2648b85256caf00731a70?OpenDocument

14. *January 14, U.S. Customs Service* — **U.S. Customs Commissioner Bonner to head U.S. delegation to OAS conference on terrorism. Customs Commissioner Robert C. Bonner will head the U.S. delegation to the Third Regular Session of the Inter−American Committee Against Terrorism (CICTE), which will take place in El Salvador January 22−24, 2003.** The conference agenda is designed to build on the momentum created by the adoption in June 2002 of the Inter−American Convention Against Terrorism, the first international legal instrument against terrorism adopted since the attacks of September 11, 2001. The meeting will expand the cooperative counterterrorism efforts undertaken thus far in the hemisphere and result in formal recommendations on counterterrorism issues to the Special Conference on Hemispheric Security planned for May. CICTE, currently chaired by the United States, is a technical body of the Organization of American States, whose basic objective is to foster multilateral cooperation in the form of training and information sharing among member nations to prevent, combat and eliminate terrorism. The United States will make a presentation on cyber security as an emerging threat and is organizing presentations on regional cooperation involving border security. **Commissioner Bonner's participation as head of the delegation reflects the United States' interest in developing a regional strategy to improve border**

security and disrupt terrorist operations throughout the Hemisphere by staunching illegal trafficking in weapons, narcotics, money, and people − all without inhibiting free trade and legitimate travel.
Source: http://www.customs.ustreas.gov/hot−new/pressrel/2003/0115−03.htm

[Return to top]

Agriculture Sector

15. *January 16, South Florida Sun−Sentinel* — **State wins appeal to resume cutting citrus trees for canker. A Florida state appeals court revived the state's citrus canker eradication law Wednesday, overturning a decision by a Broward County judge that brought the program to a near halt.** "Agriculture is second in Florida only to tourism," said Liz Compton, spokeswoman for the Department of Agriculture. "And citrus is the state's No. 1 agricultural crop. This is a win for all Florida citizens who rely on a strong economy." **The opinion stated that the citrus industry is economically important enough to justify state intervention to protect trees from the canker bacteria, which doesn't harm humans but weakens trees, causing lesions on fruit and early drop.** The Legislature enacted an eradication law that does not violate the federal or state constitutions because trees exposed to canker really do pose a threat to the citrus industry, Judge Martha Warner wrote in the appeals court decision. Owners who lose their trees can try to persuade a jury they deserve to be paid a fair price for their loss, she wrote. Opponents of the program now have three choices: they can ask the appeals court for another hearing; ask the Florida Supreme Court to overturn the decision; or bring the case back before Broward Circuit Judge J. Leonard Fleet, whose temporary order was reversed.
Source: http://www.sun−sentinel.com/news/local/broward/sfl−ccanker16jan16 ,0,7904842.story?coll=sfla−news−broward

16. *January 16, Associated Press* — **Poultry disease dooms California chickens. More than 400,000 chickens at a San Bernardino County commercial farm were ordered destroyed Wednesday after testing positive for a Exotic Newcastle disease that has forced the quarantine of Southern California's poultry.** It was the fifth commercial chicken farm hit by the disease, which is a threat to the state's $3 billion industry and forced the slaughter of more than 1.7 million chickens since it was discovered in September. The farm, which was not identified, was near backyard flocks that were infected with the disease, said Larry Cooper, spokesman for the California Department of Food and Agriculture. **California is the nation's third−largest egg producer. More than 9 million of the state's 12 million egg−laying hens are in the quarantine zone.**
Source: http://www.nytimes.com/aponline/national/AP−BRF−Poultry−Disease.h tml

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

17. *January 16, Water Tech Online* — **AMSA releases new water security software tools. The Association of Metropolitan Sewerage Agencies (AMSA) introduced two new Vulnerability Self Assessment Tools (VSAT) to help ensure that the water and wastewater critical infrastructure sector is safe and secure.** AMSA said in a news release that one is for joint water/wastewater utilities and the other is for small−to−medium sized water utilities. **VSAT water/wastewater will provide online vulnerability assessment capabilities to utilities providing both wastewater treatment and water supply services and its counterpart will do the same for both public and private water utilities, AMSA said.** The software tools were funded by the U.S. Environmental Protection Agency and are free for water and wastewater utilities. **AMSA said the tools provide a user−friendly approach to evaluate, prioritize, and remediate vulnerabilities based upon five critical utility assets: physical plant, information technology, knowledge base, employees, and customers.** AMSA is a national trade association representing hundreds of the nation's publicly owned wastewater utilities.
Source: http://www.watertechonline.com/news.asp?mode=4font>

18. *January 15, Minneapolis Star Tribune* — **Water quality programs would be affected most. Water−quality programs would be affected most by the governor's budget recommendations related to the environment, according to Minnesota state pollution−control officials.** The proposal would cut $423,000 from the Minnesota Pollution Control Agency's operating budget, which receives about $16 million annually from the state's general fund and much more from permit fees and other sources. **Cathy Moeger, the agency's chief financial officer, said most of the cuts would affect programs that identify, monitor, and clean up waters impaired by industrial, commercial, or agricultural pollution.** She said the agency would try to limit the impact by cutting administrative expenses and shifting funds from other programs. **The plan also would cut nearly $1 million from the $2.3 million that the agency receives annually for its Clean Water Partnership Grant Program. It gives grants and loans to local governments to identify water−quality problems and for cleanup.**
Source: http://www.startribune.com/stories/587/3592375.html

[Return to top]

Public Health Sector

19. *January 16, CNN* — **Scientist to appear in court in plague case. The scientist accused of making false statements about missing vials of bacteria that could cause bubonic plague is expected in court Thursday morning, law enforcement sources said.** Dr. Thomas Butler, 61, chief of the Infectious Disease Division at Texas Tech University's Department of Internal Medicine, was leading a study aimed at developing antibiotics to fight the plague. **One law enforcement source said it was Butler who notified the school Tuesday that about 30 vials were missing, prompting fears of a potential bioterror threat. Those fears, however, were short−lived, and authorities said all of the vials had been accounted for Wednesday.** Butler repeated this assertion when the FBI questioned him, saying he did not know how or why the

vials came to be missing, but he later recanted and admitted destroying them himself, the source said. Butler faces charges of making false statements to the FBI. **The vials were destroyed sometime before January 11, sources said, and Butler allegedly did not fill out the required documentation.**
Source: http://europe.cnn.com/2003/US/Southwest/01/16/missing.plague/

20. *January 15, BBC News* — **Nose drops to tackle plague threat. Scientists have developed nose drops that may help to stop a new epidemic of bubonic plague.** Experts fear the bacterium that causes bubonic plague is becoming resistant to antibiotics, and that the disease could re−establish itself across the world. **A team from the University of Birmingham, in the United Kingdom, has developed a new vaccine that can protect mice from the disease. They said that they believe a nasal spray based on the vaccine could also protect humans.** Bubonic plague, the disease that wiped out a third of Europe's population in the 14th century, is caused by a bacterium called Yersinia pestis which is spread by fleas on rodents. Up to 2,000 cases of the disease are still reported worldwide every year. **The disease can be treated with antibiotics but they must be given within 18 hours of infection. Last year, doctors in Madagascar reported plague bacteria carrying five antibiotic resistant genes, raising the possible of a drug−resistant strain. The only vaccine currently licensed for plague, which consists of killed bacteria, is only effective for half its recipients.**
Source: http://news.bbc.co.uk/1/hi/health/226546.stm

[Return to top]

Government Sector

21. *January 16, Wall Street Journal* — **For U.S., nuclear arms move to the center stage of policy.** Nuclear arms are rapidly moving to the center of America's national−security agenda. The nightmare scenario: They bring destructive powers to a terrorist or nation that would otherwise be outgunned by the U.S. military. This scenario seemed far away when President Bush first came to office and focused more on building missile defenses and doing away with arms−control treaties deemed to be relics of the Cold War. **The tense standoff with North Korea is the most immediate flashpoint, but it raises dangers that ripple far beyond the Korean peninsula. A revival of North Korea's nuclear program would add to the one or two nuclear weapons Pyongyang is believed to have already. It also would put an ever−increasing amount of nuclear material in the hands of an unstable regime that is a prime exporter of weapons with a long client list including such states as Pakistan, Iran, Libya, Syria and most recently Yemen. The Korean standoff also raises the danger that other anti−American states −− notably Iran −− will conclude that North Korea's nuclear brinkmanship has paid off by opening the door to direct talks with the U.S., tempting them to follow the same path to win respect. U.S. officials disclosed last month that they have evidence that Iran has been secretly working on two nuclear installations that could be used to produce material for nuclear warheads.** The prospect of nuclear advances in North Korea and Iran is particularly troubling, because it would signal that the danger is spreading specifically to countries that are avowedly anti−American and less sensitive to international pressure than nations such as Brazil and Argentina that flirted with nuclear arms in the past. **All told, the global picture is strikingly different from that of the 1980s and 1990s, when a wide range of countries were pressured or cajoled to forgo nuclear weapons. Using**

a combination of economic incentives and diplomatic pressure, the U.S. and its allies persuaded Argentina, South Africa, Brazil, Kazakhstan and Ukraine to give up their nuclear weapons or ambitions. For the Bush administration, the problem may require scrambling for new strategies and tools. Secretary of State Colin Powell says his top worry isn't the nations that are seeking arms, or even those such as Pakistan, which several years ago tested its nuclear weaponry in an effort to keep up with neighboring and nuclear−armed India. "I don't expect either India or Pakistan to give up their nuclear capabilities," Powell says, acknowledging that the world sees little point in trying to reverse that bit of proliferation. **Instead, he says in an interview, "the real problem is nonstate actors. And if you start to have regimes such as North Korea and Iraq and Iran that might actually have the capacity to not only make what they want, but to also provide materials to others who might not be states, but nonstate actors, that would be terrorist organizations. That's why nonproliferation efforts will still be a high priority for the administration."**
Source: http://online.wsj.com/article/0,,SB104266810269483824,00.html

22. *January 16, Washington Post* — **Commercial devices could fuel 'Dirty Bombs'; report outlines threat from lax controls.** Tens of thousands of radioactive devices currently used in medicine and industry are powerful enough to inflict major damage if used by terrorists in a "dirty bomb," yet governments worldwide have failed to take steps needed to prevent them from falling into the wrong hands, according to a study scheduled for release today. **Despite a growing awareness of dirty bombs, U.S. law places few limits on exports of radioactive equipment, even to troubled states such as Afghanistan or the former Soviet republics, says the report by the Center for Nonproliferation Studies at Monterey Institute of International Studies. Dirty bombs are crude weapons that use conventional explosives to spread dangerous radiation.** Lax controls have left a legacy of thousands of lost and abandoned radioactive devices around the world, especially in the former Soviet Union. "The locations of many unauthorized dumps of radioactive sources remain unknown," the report says. The study, the result of a yearlong investigation, is among the first to examine security risks posed by commercial radioactive equipment. The risks involve only a small fraction of the millions of commercial radioactive devices manufactured since the 1940s −− a finite number of highly radioactive machines and tools that could be quickly identified and secured if governments acted aggressively to fix the problem, the study's authors said. A half−dozen nations produce the vast majority of radioactive equipment that poses the greatest threat, they said. **The Monterey report calls for tighter controls on exports of radioactive equipment and better oversight of the use and eventual disposal of the devices. It calls for improved international efforts to round up radioactive devices that have been abandoned or illegally dumped. An Energy Department initiative that recovered 10,000 "orphaned" devices in recent years is being threatened this year with deep funding cuts, the study notes.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A63720−2003Jan15.ht ml

[Return to top]

Emergency Services Sector

23. *January 16, New York Times* — **New York police send an investigator to London to focus on a poison threat.** The New York Police Department has sent a senior counterterrorism official to London because of concerns about the threat posed by a group of North African men

accused of plotting terrorist attacks there using the lethal toxin ricin, and the department may send additional investigators, according to New York and British police officials. **Both the New York Police commissioner, Raymond W. Kelly, and the head of the Metropolitan Police in London, Sir John Stevens, said the move was part of a broader effort to exchange intelligence between the two cities, which share similar concerns about global terrorism, including biological weapons. The two men discussed the arrangement at a meeting in New York City on Jan. 8, they said. While there appear to be no connections between the London case and New York City, both officials said the two departments could learn a great deal from each other. Kelly made his comments in an interview yesterday and Sir John made his in an interview last week in New York.** "We're concerned about the knowledge these people have and any contacts in the U.S. they may have," Kelly said. "Big cities — Paris, New York, London — have a bond as far as being targeted by terrorists, and we have to continue to exchange information and, indeed, increase our exchange of information."
Source: http://www.nytimes.com/2003/01/16/nyregion/16RICI.html

[Return to top]

Information and Telecommunications Sector

24. *January 17, CERT Coordination Center* — **ISC has discovered several buffer overflow vulnerabilities in their implementation of DHCP (ISC DHCPD). These vulnerabilities may allow remote attackers to execute arbitrary code on affected systems.** There are multiple remote buffer overflow vulnerabilities in the ISC implementation of DHCP. As described in RFC 2131, "the Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network." In addition to supplying hosts with network configuration data, ISC DHCPD allows the DHCP server to dynamically update a DNS server, obviating the need for manual updates to the name server configuration. Support for dynamic DNS updates is provided by the NSUPDATE feature. During an internal source code audit, developers from the ISC discovered several vulnerabilities in the error handling routines of the minires library, which is used by NSUPDATE to resolve hostnames. These vulnerabilities are stack−based buffer overflows that may be exploitable by sending a DHCP message containing a large hostname value. Note: Although the minires library is derived from the BIND 8 resolver library, these vulnerabilities do not affect any current versions of BIND. A solution is posted at the source site.
Source: http://www.kb.cert.org/vuls/id/284857#systems

25. *January 16, New York Times* — **Wireless services bill introduced.** Senators George Allen (R−VA) and Barbara Boxer (D−CA), have introduced legislation to promote wireless broadband deployment. **The bill,the Jumpstart Broadband Act, calls for the Federal Communications Commission to allocate at least 255 megahertz of spectrum in the 5−gigahertz band for unlicensed use by wireless broadband services**. The measure seeks to **support the expansion of wireless technology known as WiFi, which allows users of personal and hand−held computers to connect to the Internet at high speed without cables**. Allen said the legislation would create an environment that embraces innovation and encourages the adoption of next−generation wireless broadband Internet devices. In addition, he said, such action would build confidence among consumers, investors and those in the

telecommunications and technology industries.
Source: http://www.nytimes.com/2003/01/16/technology/16TBRF3.html

26. *January 16, Government Computer News* — **FedCIRC prepares to launch new security patch service. The Federal Computer Incident Response Center introduced systems and security administrators to its new patch distribution service today**. Mark Forman, associate director for IT and e−government at the Office of Management and Budget, said **the Patch Authentication and Dissemination Capability could help agencies meet requirements of the Federal Information Security Management Act**. The General Services Administration's FedCIRC is offering PADC as a free service to civilian agencies. SecureInfo Corp. of San Antonio and Veridian Corp. of Arlington, Va., developed it under a $10.8 million, five−year task order. It is expected go online next week. Agencies with accounts will enter hardware and software profiles of their systems and be told what security vulnerabilities they face and what patches or other fixes they will need to correct them. Users also will be alerted to new vulnerabilities that could affect their systems. Patches will be validated and tested by Veridian, then digitally signed and stored on a secure server by SecureInfo. **The goal is to simplify patch management by providing administrators only with information relevant to their IT systems and ensuring that patches are genuine and effective**.
Source: http://www.gcn.com/vol1_no1/daily−updates/20885−1.html

27. *January 16, International Data Group* — **Security flaw found in Microsoft's Windows Powered Smartphone software.** Microsoft and mobile phone operator Orange are working to patch a security bug that affects the first mobile phone to use Microsoft's Windows Powered Smartphone software, Orange said Thursday. **The SPV phone can run downloadable applications. It was designed to only run certified applications, in order to protect customers against rogue code**. However, **details on how to disable this security feature have become public, allowing the installation of applications that have not been certified**. **Microsoft and Orange have investigated the issue and will provide a security update as soon as possible to solve it**, Orange said. **Users will be able to download this update through the Orange Update application on their SPV**. Because changes have to be made directly on the phone to be able to bypass the security, Orange said it does not see the issue "as posing any risk to the security" of SPV users.
Source: http://www.pcworld.com/news/article/0,aid,108834,00.asp

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 www.securityfocus.com

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **PE_FUNLOVE.4099** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 80 (http), 1433 (ms−sql−s), 21 (ftp), 53 (domain), 4662 (???), 139 (netbios−ssn), 135 (???), 27374 (asp), 443 (https) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

28. *January 16, New York Times* — **Swiss plan tight security and no−flight zone at economic talks.** The Swiss government ordered army protection today for participants in the World Economic Forum in Davos next week, announcing it would send up to 2,000 soldiers, create a no−flight zone there, and empower the military to shoot down unauthorized aircraft. **In one of the tightest security moves in Switzerland's history, the government has authorized spending a record $2.3 million to protect the more than 1,000 corporate chiefs, 250 political leaders, 200 media executives and 200 prominent social activists expected to attend the annual meeting in Davos, a fashionable ski village in the Swiss Alps. Davos has been the forum's home since the event began 33 years ago, except for last year, when it was held in New York.** Livio Zanolari, a government spokesman, said the measures were not a response to any specific terrorist threat. Rather, he said, it reflected the government's caution and concern for the participants, who will include Secretary of State Colin L. Powell and Brazil's new president, Luiz Inácio Lula da Silva. The Swiss Army is also lending the forum 10 helicopters, which will be used to patrol the air space in the area as well as to shuttle top officials to Davos from Zurich's international airport. Soldiers from neighboring Liechtenstein will also be guarding the forum, in addition to hundreds of police from throughout Switzerland. German soldiers are on alert status. Switzerland has also granted 100 foreign security officers and personal bodyguards temporary permission to use firearms.
Source: http://www.nytimes.com/2003/01/16/international/europe/16DAVO.htm l

29. *January 16, New York Times* — **U.S. to seek extradition of two in Germany on possible al Qaeda ties.** Officials in the United States and in Germany confirmed on Wednesday that the arrest of the two men, Sheik Muhammad Ali Hassan al−Mouyad and Muhammad Moshen Yahya Zayed, stemmed from charges filed this month in the Eastern District of New York alleging they provided support to a terrorist organization. **The federal Department of Justice notified Germany yesterday that it would seek to extradite the men to the United States, a United States Embassy spokesman said.** A spokesman for the United States attorney's office in Brooklyn had no immediate comment on the charges, which remain under seal. **Sheik Mouyad is thought to be an al Qaeda financier who used a home base in the Yemeni capital, Sana, to collect money for the terrorist organization, according to a United States official who spoke on the condition of anonymity. Zayed, Sheik Mouyad's traveling companion, is said to have played a lesser role in the organization. Sheik Mouyad's family and political allies called his arrest a mistake, saying the United States government relied on flawed information and faulty investigative techniques.** The two men were arrested last Friday at a hotel near the Frankfurt airport and are being held at a nearby maximum security

prison. They were ordered held pending extradition.
Source: http://www.nytimes.com/2003/01/16/nyregion/16BROO.html

[Return to top]

NIPC Products &Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web−site (http://www.nipc.gov), one can quickly access any of the following NIPC products:

NIPC Advisories − Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

NIPC Alerts − Alerts address major threat or incident information addressing imminent or in−progress attacks targeting specific national networks or critical infrastructures.

NIPC Information Bulletins − Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

NIPC CyberNotes − CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure−related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:	Melissa Conaty (202−324−0354 or mconaty@fbi.gov) Kerry J. Butterfield (202−324−1131 or kbutterf@mitre.org)
Distribution Information	NIPC Watch and Warning Unit (202−323−3204 or nipc.watch@fbi.gov)

NIPC Disclaimer